Office of the Governor
State Chief Information Officer

SECURITY

Chapter 12 – Complying with Legal and Policy Requirements

Scope: These policies apply to all public agencies, their agents or designees subject to Article 3D of Chapter 147, "State Information Technology Services."

Statutory Authority: G.S. §147-33.110

Section 01 Complying with Legal Obligations

120101 Being Aware of Legal Obligations

Purpose: To ensure that employees are familiar with the laws that govern use of information technology systems and the data contained within those systems.

STANDARD

Agencies shall ensure that all employees and contractors are aware of legal and regulatory requirements that address the use of information technology systems and the data that reside on those systems.

Agencies also must ensure that each public employee and other State Network user is provided with a summary of the legal and regulatory requirements before or at the same time that the employee or other State Network user is provided initial access to the State Network.

Examples of laws that affect computer and telecommunications use in North Carolina

- **Federal**
  - 18 U.S.C. §1030. Fraud and related activity in connection with computers.
  - 17 U.S.C.§§ 500 and 506. Copyright infringements and remedies.
- **North Carolina**
  - N.C.G.S. §114-15.1. Misuse of state property.
  - N.C.G.S. §14-196. Using profane, indecent or threatening language to any person over the telephone; annoying or harassing by repeated telephoning or making false statements over telephone. The statute includes the sending by computer

modem of any false language concerning death, injury, illness, disfigurement, indecent conduct or criminal conduct of the person receiving the information or any close family member.

- N.C.G.S. §14-454. Accessing computers.
- N.C.G.S. §14-455. Damaging computers, computer systems, computer networks, and resources.
- N.C.G.S. §14-457. Extortion.
- N.C.G.S. §14-458. Computer trespass; penalty.
- N.C.G.S. §14-155. Unauthorized connections with telephone or telegraph.

Examples of laws that affect data residing on State information technology systems

- Federal
  - 26 U.S.C. §§6103, 7213, 7213A, 7431, Internal Revenue Code.
  - Public Law 104-191, 104th Congress, Health Insurance Portability and Accountability Act of 1996.
  - 5 U.S.C. §552a, as amended. Privacy Act of 1974.
- State
  - N.C.G.S. Chapter 132. Public records law.
  - N.C.G.S. §105-259. Secrecy required of officials.
  - N.C.G.S. §122C-52. Client rights to confidentiality.

Additional laws that relate to confidential records in North Carolina are summarized at: http://www.ah.dcr.state.nc.us/records/guides/confidential_public-rec_statutes_2006.pdf.

ISO 17799: 2005 References
8.1.3 Terms and conditions of employment
15.1.1 Identification of applicable legislation

120102 Complying with State and Federal Records Laws

Purpose: To ensure that agencies comply with laws that address proper handling of datacontained in information technology systems.

STANDARD

State agencies are subject to State laws governing the use of information technology systems and the data contained in those systems. In some situations, State agencies are also subject to federal laws. Agencies shall take affirmative actions to comply with all applicable laws and take measures to protect the information technology systems and the data contained within information systems.

ISO 17799: 2005 References
15.1.4 Data protection and privacy of personal information

120103 Complying with General Copyright Laws

Purpose: To ensure that agencies comply with laws that address copyright protection.

STANDARD

Agencies shall provide employees with guidelines for obeying software licensing agreements and shall not permit the installation of unauthorized copies of commercial software on technology devices that connect to the State Network.

The guidelines shall inform employees that:

- Persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties.
- Employees shall obey licensing agreements and shall not install unauthorized copies of commercial software on State agency technology devices.
- State employees who make, acquire or use unauthorized copies of computer software shall be disciplined as appropriate. Such discipline may include termination.

ISO 17799: 2005 References
15.1.1 Identification of applicable legislation

120104 Complying with Database Copyright Law

Purpose: To ensure that agencies comply with laws that address copyright protection

STANDARD

Agencies shall inform their employees of any proprietary rights in databases or similar compilations and the appropriate use of such data. Agencies shall also inform employees of any sanctions that may arise from inappropriate use of the databases or similar compilations.

ISO 17799: 2005 References
15.1.2 Intellectual property rights (IPR)

120105 Complying with Copyright and Software Licensing Requirements

Purpose: To ensure that agencies comply with copyright and licensing requirements.

STANDARD

Each agency shall establish procedures for software use, distribution and removal within the agency to ensure that agency use of software meets all

copyright and licensing requirements. The procedures shall include the development of internal controls to monitor the number of licenses available and the number of copies in use.

ISO 17799: 2005 References
15.1.2 Intellectual property rights (IPR)

120106 Legal Safeguards against Computer Misuse

Purpose: To disclose to users of State information systems the legal policy requirements for using State information technology resources as well as any methods an agency may use to monitor usage.

STANDARD

Agencies shall provide users of information technology services with the legal policy requirements that apply to use of State information technology systems and, where practical and appropriate, agencies shall provide notice to users of State information technology systems that they are using government computer systems.

If agencies monitor computer users, agencies also shall provide notice to computer users that their activities on State information technology systems may be monitored and disclosed to third parties.

GUIDELINES

The notice required by this standard can take many forms. An Internet Web page may have a link to a privacy statement. Monitoring notices can consist of stickers pasted to a computer monitor or an electronic notice that displays when the user logs on to a computer. Where practical and appropriate, sign-on warning banners shall be posted on State government computer systems to appear just before or just after login on all systems that are connected to the State Network, giving notice to users that they are accessing State resources and that their actions while they are using these resources may be subject to disclosure to third parties, including law enforcement personnel.

Examples of warning banners:

- WARNING: This is a government computer system, which may be accessed and used only for authorized business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil and/or administrative action.
- All information on this computer system may be intercepted, recorded, read, copied and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system.
- NOTICE: This system is the property of the State of North Carolina and is for authorized use only. Unauthorized access is a violation of

federal and State law. All software, data transactions and electronic communications are subject to monitoring.

- This is a government system restricted to authorized use and subject to being monitored at any time. Anyone using this system expressly consents to such monitoring and to any evidence of unauthorized access, use or modification being used for criminal prosecution and civil litigation.
- *Notice to Users.* This is a government computer system and is the property of the State of North Carolina. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.
- Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected and disclosed to law enforcement personnel, as well as to authorized officials of other agencies. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection and disclosure at the discretion of the Office of Information Technology Services.
- Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

ISO 17799: 2005 References
15.1.5 Prevention of misuse of information processing facilities

---

Section 02 Complying with Policies

120201 Managing Media Storage and Record Retention

Purpose: To establish standard for records retention and disposition.

STANDARD

For the records they create or receive in the course of performing the public's business, agencies are required to formulate complete and accurate record retention and disposition schedules that comply with the provisions of N.C.G.S. §§121-5 and 132-1, *et seq.* Agencies must manage their records according to the schedules, as approved by the Department of Cultural Resources, State Records Branch, throughout the records' life cycle, from creation to disposition.

ISO 17799: 2005 References
15.1.3 Protection of organizational records

120202 Complying with Information Security Standards and Policy

Purpose: To establish security standards and policy compliance requirements for employees.

STANDARD

Agencies shall establish requirements for mandatory compliance with the applicable statewide and individual agency information technology security standards and policies. The requirements shall include regular policy and standard reviews for employees and contractors and periodic reviews of information technology systems to determine whether the systems are in compliance with applicable policies and standards.

ISO 17799: 2005 References
8.1.3 Terms and conditions of employment
15.2.1 Compliance with security policies and standards

Section 03 Avoiding Litigation

120301 Safeguarding against Libel and Slander

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

120302 Using Copyrighted Information from the Internet

Purpose: To comply with applicable copyright laws.

STANDARD

Agencies shall seek legal review before using copyrighted information.

ISO 17799: 2005 References
15.1.2 Intellectual property rights (IPR)

120303 Sending Copyrighted Information Electronically

Purpose: To comply with applicable copyright laws.

STANDARD

Agencies shall seek legal review before sending copyrighted information electronically.

ISO 17799: 2005 References
15.1.2 Intellectual property rights (IPR)

120304 Using Text directly from Reports, Books or Documents

Purpose: To comply with applicable copyright laws

STANDARD

Agencies shall seek legal review before using copyrighted information contained in reports, books and documents.

ISO 17799: 2005 References
15.1.2 Intellectual property rights (IPR)

120305 Infringement of Copyright

Agencies should address the standard set forth in the ISO 17799 Security Standard with agency legal counsel.

GUIDANCE

See, Using the Internet for Work Purposes 030312

ISO 17799: 2005 References
15.1.2 Intellectual property rights (IPR)

Section 04 Other Legal Issues

120401 Recording Evidence of Information Security Incidents

Purpose: To create formal records of information technology security incidents.

STANDARD

Agencies shall record information technology security incidents on the Incident Reporting form,[1] incorporated by reference.

GUIDELINES

Agencies shall also establish formal procedures for recording and retaining evidence relating to information security incidents to ensure that the evidence is properly preserved for any legal actions that may ensue as a result of the incidents.

ISO 17799: 2005 References
10.10.1 Audit logging
10.10.2 Monitoring system use
13.1.1 Reporting information security events
13.2.3 Collection of evidence
15.1 Compliance with legal requirements

[1] The Incident Reporting form can be found at https://incident.its.state.nc.us/ and can be filled out online.

120402 Renewing Domain Name Licenses –Web Sites

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

120403 Insuring Risks

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

120404 Recording Telephone Conversations

Purpose: To establish procedures to follow when recording telephone conversations.

STANDARD

Each agency shall establish policies for recording telephone conversations that describe the circumstances under which a telephone conversation may be recorded, any notification that will be provided to the individual being recorded, and the procedures for maintaining the records of those conversations.

ISO 17799: 2005 References
10.8.1 Information exchange policies and procedures
15.1.1 Identification of applicable legislation

120405 Admissibility of Evidence

Agencies should address the standard set forth in the ISO 17799 Security Standard with agency legal counsel.

ISO 17799: 2005 References
13.2.3 Collection of evidence

120406 Adequacy of Evidence

Agencies should address the standard set forth in the ISO 17799 Security Standard with agency legal counsel.

ISO 17799: 2005 References
13.2.3 Collection of evidence

120407 Reviewing System Compliance Levels

Purpose: To provide that systems are regularly reviewed for compliance with security requirements.

STANDARD

Information systems shall be regularly reviewed for compliance with security standards. The compliance review should be performed by qualified information technology personnel and/or with the assistance of automated tools.

When penetration tests or vulnerability assessments are used, agencies must follow the requirements of G.S. §147-33.111(c).

RELATED INFORMATION

G.S. §147-33.111(c)

ISO 17799: 2005 References
15.2.2 Technical compliance checking

120408 Collection of Evidence

Agencies should address the standard set forth in the ISO 17799 Security Standard with agency legal counsel.

ISO 17799: 2005 References
13.2.3 Collection of evidence

HISTORY (HISTORY TITLE)

State CIO Approval Date: March 22, 2006
Original Issue Date: March 22, 2006
Subsequent History:

Standard Number	Version	Date	Change/Description

Old Security Policy/Standard	New Standard Numbers
Policy and Guidelines for Developing Privacy Policies for Users of State Information Systems	120106 – Legal Safeguards against Computer Misuse. *See also,* Privacy.
Notification Banner Policy and Guidelines	120106 – Legal Safeguards against Computer Misuse. *See also,* Privacy
Incident Management Policy	120401 Recording Evidence of Information Security Incidents
Incident Response Standard	120401 – Recording Evidence of Information Security Incidents.